Function_map section 620, represents functions supported on a given platform. In one embodiment, as indicated by reference number 621, the data in the function map appears as ordered pairs of integers. In one embodiment, the first integer is a generic external representation of the function as provided in the function_list section (described above), and the second integer is an internal representation of the event that may differ depending upon the particular platform involved.

(2) On page 30, please replace the paragraph from line 14 through line 5 of page 31 with:

Like the RMCP header section, RMCP data section 830 also contains various fields including: event code field 832, data length field 834, checksum field 836, and data field 839. Event code field 832 contains data that indicates the type of event that has occurred on the client as explained above with respect to Figures 4A, 4B and 5. If event code field 832 indicates that a "simple" event "1" has occurred, the alert proxy references the Event_map section of its description file to determine an appropriate direct event mapping. Data length field 834 is used to indicate the length of the RMCP data section that follows. In one embodiment, data length field 834 is assigned a fixed value representing a length of 46 bytes. Checksum field 836 appears in both the RMCP transmit packet format and receive packet format, but is implemented differently in each. In the RMCP transmit data packet, the UDP checksum is used by the system rather than an RMCP-specific checksum that utilizes checksum field 836. In transmit mode therefore, the value of checksum field 836 is set equal to zero since the field remains unused. Data field 839 may contain data that provides additional event descriptions to be parsed and used by the alert proxy.

Currently Pending Claims

1   1.   In a client device, a method comprising:

2   receiving externally provided control operations;

3   determining a current operating state of said client device; and

4   conditionally executing said control operations if execution of said control operations are

5   permitted while said client device is in said determined current state.

1 2.   The method of claim 1, wherein receiving externally provided control operations includes

2 receiving a system reset operation.

1 3.   The method of claim 1, wherein receiving externally provided control operations includes

2 receiving a system power operation.

1 4.   The method of claim 1, wherein said externally provided control operations are received

2 from a server device coupled to said client device over a network.

1 5.   The method of claim 1, wherein said current operating state of said client device is

2 determined by inspecting at least one status register on said client.

1 6.   The method of claim 1, wherein said control operations are permitted while said client

2 device is in a system hung state.

1 7.   The method of claim 1, wherein said externally provided control operations are received via

2 a network data packet encapsulated according to a remote management and control protocol

3 (RMCP).

1 8.   An apparatus comprising:

2   a first electronic component;

3   a bus;

4   a sensor coupled to said bus and said first electronic component; and

5   a second electronic component coupled to said bus to conditionally cause said first

6   electronic component to perform a plurality of functions through said sensor, via said bus,

7   responsive to externally provided control operations.

1   9.   The apparatus of claim 8, wherein said first electronic component further comprises a

2   reset pin, and wherein said second electronic component coupled to said bus conditionally causes

3   said first electronic component to perform a reset function.

1   10.   The apparatus of claim 9, wherein said first electronic component includes a processor.

1   11.   The apparatus of claim 8, wherein said bus includes a system management bus.

1   12.   The apparatus of claim 8, further comprising a network controller.

1   13.   The apparatus of claim 12, wherein said external control operations are provided by a

2   server device connected to said apparatus through said network controller.

1   14.   The apparatus of claim 8, further comprising:

2   an operating system; and

3   a processor to execute said operating system.

1   15.   The apparatus of claim 14, wherein said second electronic component conditionally

2   causes said first electronic component to perform said plurality of functions prior to said

3   operating system having been executed by said processor.

1   16.   The apparatus of claim 8, wherein said externally provided control operations are

2   encapsulated in a remote management and control protocol (RMCP) formed data packet.

1   17.   In a server, a method comprising:

2   providing a first re-boot command to a remote client device to re-boot said remote client

3   device to a first operational state;

4   determining if said remote client device was successful in re-booting to said first

5   operational state; and

6   providing a second re-boot command to said remote client device to re-boot said remote

7   client device to a second operational state, if said remote client device was unsuccessful in re-

8   booting to said first operational state.

1   18.   The method of claim 17, wherein said at least one of said first and second re-boot

2   commands are provided to said remote client while said remote client is in an operating system

3   unavailable state.

1   19.   The method of claim 18, wherein said operating system unavailable state includes an

2   operating system hung state.